(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 January 2005 (06.01.2005)

PCT

(10) International Publication Number
WO 2005/002131 A1

(51) International Patent Classification[7]: H04L 9/14

(21) International Application Number: PCT/KR2004/001569

(22) International Filing Date: 28 June 2004 (28.06.2004)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
10-2003-0042611 27 June 2003 (27.06.2003) KR

(71) Applicant *(for all designated States except US)*: **KT Corporation** [KR/KR]; 206, Jungja-dong, Bundang-gu, Seongnam-city, Kyeongki-do, 463-711 (KR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PARK, Young-Man** [KR/KR]; Mido Apt. 102-210, Sanggye 6-dong, Nowon-gu, Seoul 139-904 (KR). **LEE, Seong-Choon** [KR/KR]; Mido Apt. 106-204, Daechi-dong, Kangnam-gu, Seoul 135-775 (KR). **TCHA, Yong-Joo** [KR/KR]; Cheongsol-maeul Hwain Apt. 204-303, Geumgok-dong, Bundang-ku, Seongnam-city, Kyungki-do 463-720 (KR).

(74) Agent: **YOU ME PATENT AND LAW FIRM**; Seolim Bldg.,, 649-10 Yoksam-dong,, Seoul 135-080 (KR).

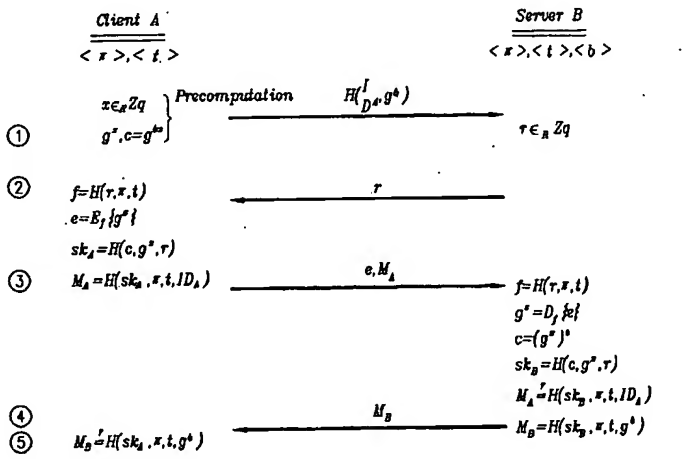
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: TWO-FACTOR AUTHENTICATED KEY EXCHANGE METHOD AND AUTHENTICATION METHOD USING THE SAME, AND RECORDING MEDIUM STORING PROGRAM INCLUDING THE SAME



(57) Abstract: A two-factor authenticated key exchange method. A subscriber station transmits a value generated by using an identifier and an authentication server's public key to the authentication server through an access point. The authentication server uses the value to detect the subscriber's password, a key stored in a token, and the authentication server's secret key, generate a random number. The subscriber station uses the random number, password, and the key to transmit an encrypted value and the subscriber's authenticator to the authentication server. The authentication server establishes a second value generated by using the password, key, and random number to be a decrypted key to decrypt the encrypted value, authenticate the subscriber's authenticator, and transmits the authentication server's authenticator to the subscriber station. The subscriber station authenticates the authentication server's authenticator by using the key and password.

WO 2005/002131 A1